AIR WAR COLLEGE

AIR UNIVERSITY

ACHIEVING MISSION ASSURANCE AGAINST A CYBER THREAT WITH THE DEFENSE ACQUISITION SYSTEM

by

Robert T. Ungerman III, Lieutenant Colonel, United States Air Force

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Chad Dacus

13 February 2016

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lieutenant Colonel Robert Ungerman is assigned to the Air War College, Air University, Maxwell AFB, AL. After graduation from the Reserve Officer Training Corps at Embry-Riddle Aeronautical University in Daytona Beach, FL, he attended pilot training at Sheppard AFB, TX. From there he served as a T-38 instructor pilot and went on to fly F-16s at Hill AFB, UT. There he deployed in support of Operation IRAQI FREEDOM and was subsequently selected for the US Air Force Test Pilot School at Edwards AFB, CA. Following graduation, he served in numerous positions executing F-16 flight test and test support for numerous current and future Air Force weapon systems. Prior to attending Air War College, Lieutenant Colonel Ungerman served as Commander of the 416th Flight Test Squadron where he oversaw the planning, execution, and reporting of more than 40 upgrades to F-15, F-16, and T-38 aircraft for the US and her allies.

Abstract

Most DOD major weapon systems were designed before 1990 and were never deemed susceptible to a "hacking" threat. Decades of subsequent engineering focused on information *availability and usability* rather than *security*. Today we are left with a fleet of aircraft operating in a system of systems that has much vulnerability and little cyber hardening. Current guidance is not sufficient to obtain mission assurance, and without clarification, the DOD cannot assure mission success in the face of cyber threats.

The author argues that three major guidance changes are needed. First, a functional mission analysis (FMA) should be conducted on every major weapon system. This will determine (and prioritize) the *minimum* requirements and subsystems needed for critical mission execution. Identification and prioritization of these systems will enable more focused and efficient vulnerability assessments that will eventually drive mission assurance to be "baked in" to system design. Second, FMAs and vulnerability assessments should be conducted prior to every acquisition milestone. Earlier assessments (in contrast to current guidance) will allow for timely and cost-effective changes to system design. Without a change in guidance, the DOD runs the risk of finding vulnerabilities that are either too costly to fix or too unsecure to field. Lastly, the DOD must mandate the inclusion of uniquely-qualified Cyber Vulnerability Assessment (CVA) Engineers at all vulnerability assessments. The extremely limited availability of these professionals may drive (and allow) a program to conduct halfhearted assessments unless current guidance is modified.

Current direction allows a program strapped for time and money to execute (and pass) a vulnerability assessment that is too late, conducted without the proper experts, and does not address the most critical aspects of mission execution. Changes are needed.

Introduction

An Airbus A400M crashed during a test flight in Seville, Spain in May 2015. Investigators learned misconfigured engine control data caused the fatal accident.[1] Initial reports confirmed three of the four engines lost power shortly after takeoff due to missing torque calibration data that should have been installed during final aircraft assembly.[2] Other than the missing information, the aircraft was in perfect working order and the aircrew had performed flawlessly.

The Seville incident was not a cyber-attack, but the accident demonstrated that an advanced, networked, information-dependent aircraft was susceptible to the loss of integrity and availability of "cyber" information. Initial reports blamed the incident on a lapse of protocol during aircraft final assembly, but the root cause was actually poor engineering during system design. Designers should have recognized that flight was impossible without torque calibration data, and they should have implemented a control to prevent takeoff in the unsatisfactory condition. This simple measure would have saved four lives and an otherwise perfect, $192 million aircraft.[3]

As warfighters, we must ask ourselves, "could malicious actors choreograph similar catastrophic results?" Accessing and manipulating the engine data through any number of methods (i.e. network exploitation, compromised maintenance systems, etc.) could have caused similar, or potentially worse, results. Could a malicious actor corrupt fleet-wide data if standard protocol were to receive automatically updated engine information via the internet? In this case, one could imagine a number of the 174 A400Ms in use by the year 2020 crashing with little to no warning between incidents.

Configuration control of software and data presents a significant concern for many advanced systems, but the cyber threat to military aircraft engaged against an adversary is a radically more complex problem.[4] If an adversary could add, delete, or manipulate information before a flight (or during an engagement), mission success could not be assured. Those unfamiliar with the nuances of cybersecurity may propose building an enhanced firewall to prevent malicious actors from accessing a weapon system, but this is a common miscalculation that Department of Defense (DOD) leaders must quickly move past. To better understand the crisis facing US weapon systems, one should consider the cyber problem as two distinct, yet related, challenges. The first challenge is to understand *how systems and networks* are infiltrated. The second challenge is to understand *what happens to systems* when missing or incorrect information is introduced.[5,6]

Challenge #1: How is a System Infiltrated?

Identifying every method of system infiltration is a daunting task. Even if every attack vector is identified, the various methods of exploitation are left to the imagination of the attacker, as illustrated in the following examples. As a precursor to computer hacking, malicious actors discovered that presenting a 2,600 hertz tone to an open phone line allowed partial control over the line, including free long-distance services.[7] Decades later, e-mail was initially intended to allow efficient communication, but malicious actors recognized the new service was an excellent attack vector for uploading unwanted information (i.e. spyware) via harmless-looking attachments. So, just because an attack vector has been identified (i.e. open phone line, incoming e-mail, etc.) does not mean a defender can predict how an adversary will exploit it.

Securing systems with firewalls has proven ineffective time and time again. One simply considers news reports of stolen data from the Joint Strike Fighter program in 2007, Office of

Personnel Management in 2014, or other recent high-profile incidents to understand the ineffectiveness of firewalls.[8,9] In each case, despite these networks being highly defended, malicious actors were able to extract terabytes of priceless information. So if some of the world's best-defended networks have proved susceptible, is it reasonable to expect a "better" firewall on the A400M (or F-22) can assure mission success? The answer is "No." The DOD should focus on understanding *what happens* after a system is accessed rather than *how to prevent* an adversary from infiltrating the system.

Challenge #2: What Happens After Infiltration?

Missing information caused the Airbus A400M to crash. If the engine information were present but *incorrect,* would the outcome have been equally catastrophic? If design engineers fail to address these considerations during development, hopefully the shortcomings will be discovered during a test and evaluation phase. If not, the DOD could field a system with deadly failure modes that will eventually be discovered by unsuspecting users. Finding flaws in this manner is the most dangerous and costly way of vulnerability identification.

Recognizing that vulnerabilities are born during system design, one must understand how these vulnerabilities relate to mission assurance and risk. Mission assurance is the science of ensuring effectiveness in the face of an adversary's best effort, whether that is by cyber or other means. Overall mission risk due to a cyber-intrusion is a function of threat, vulnerability, and impact:

$$Mission\ Risk\ \equiv\ f(threat)\ *f(vulnerability)*f(impact)$$ [10]

If no threat exists, there is no risk of an intrusion, thus no risk to the mission. Similarly, if there is no negative impact after an actor infiltrates and modifies information, there is no mission risk. Short of war, the DOD cannot eliminate the existence of a threat but *can* attempt to

manage the "vulnerability" and "impact" variables. This is accomplished by first identifying vulnerabilities within the system, then modifying the design (or tactics, techniques, and procedures) to either mitigate mission impact or eradicate the vulnerability. Driving this risk equation towards zero is the essence of mission assurance. In summary, the DOD must mitigate vulnerabilities from the *inside*, rather than solely focus on stopping the adversary from accessing the system from the *outside*.

Thesis

Vulnerability assessments are broadly outlined in current directives, but additional guidance is needed to clarify the steps, timing, and personnel requirements related to these assessments. First, a requirement for execution of a functional mission analysis (FMA) on each system is needed. Next, vulnerability assessments and FMAs should be conducted before each milestone. Lastly, and most importantly, updated guidance should mandate the inclusion of unique cyber subject matter experts (SMEs) "educated in the science of information assurance and trained in the art of cyber warfare" for all cyber hardening (CH) events.[11,12] Future vulnerability assessments have a high likelihood of failure without these modifications to current guidance.

This research paper will first introduce the problem facing DOD weapon systems and review current acquisition guidance related to cyber testing and evaluation. The author will then describe the importance of instituting FMAs and follow with a description of the basic tenets and timing of CH events. Lastly, an explanation of major actors within the CH team will focus on the mandatory inclusion of Cyber Vulnerability Assessment (CVA) Engineer.

Background

Most DOD major weapon systems were designed before 1990. While computer hacking sprung to front page news in the 1980s, military aircraft were not determined susceptible to the hacking threat. Decades of subsequent engineering focused on information *availability and usability* rather than *security*. Today we are left with a fleet of aircraft operating in a system of systems that has much vulnerability and offers little cyber hardening. Considering the stakes with incredibly destructive and expensive weapon systems, the DOD should take immediate action to identify and mitigate cyber vulnerabilities in currently-fielded and future platforms.

Virtually all modern aircraft have some components that interact with a larger network, such as the internet, classified and unclassified government networks, or contractor managed (and protected) networks. System components exposed to these networks may include mission planning software, data transfer hardware, maintenance systems, and unclassified CDs with upgraded software for auxiliary equipment. From this wide array of potential cyber "attack vectors," one can understand that overall system security is not simply a function of protecting the physical aircraft, but rather extends to all networks and subsystems required by the overall system. Our ability to keep the adversary "out" is not a viable option for mission assurance. We must assume the adversary will gain access and have the ability to add, delete, or modify information within the system. Maybe access allows an introduction of malware, or maybe it allows deletion of engine data. In any case, system design must assure mission accomplishment despite being compromised by an adversary. US warfighters must be allowed to "fight hurt."

Current Guidance and Efforts

Current DOD instructions have provided a roadmap for acquisition program managers (PMs) to operate without specific cyber requirements, but there exists too much leeway in the

guidance. Currently, it's reasonable to think a well-intentioned PM could bypass the rigor required of vulnerability assessments in the name of reducing cost and meeting schedule. After all, the PM does not have specific "cyber requirements" to spend the program's money against. A brief look at current guidance is necessary to better understand the excessive flexibility.

All DOD acquisition programs are governed by DODI 5000.02, *Operation of the Defense Acquisition System*. This instruction dictated that programs using information technology (IT) shall develop a cybersecurity strategy and that developmental test and evaluation (DT&E) "should include activities to detect cyber vulnerabilities," but it did not specify *how* to conduct these vulnerability assessments.[13] Further DOD direction was published in the March 2014 release of DODI 8500.01, *Cybersecurity*. This publication mandated that cybersecurity assessments be integrated into developmental and operational testing and that a cybersecurity representative must be present. Unfortunately the instruction failed to specify the timing of the assessments and the qualifications of the cybersecurity representative.[14] To partially fill the void of specific guidance, Undersecretary of Defense for Acquisition, Technology, and Logistics published the *Cybersecurity Test and Evaluation* [T&E] *Guidebook* in July 2015 and divided cybersecurity testing into six major phases (Figure 1).

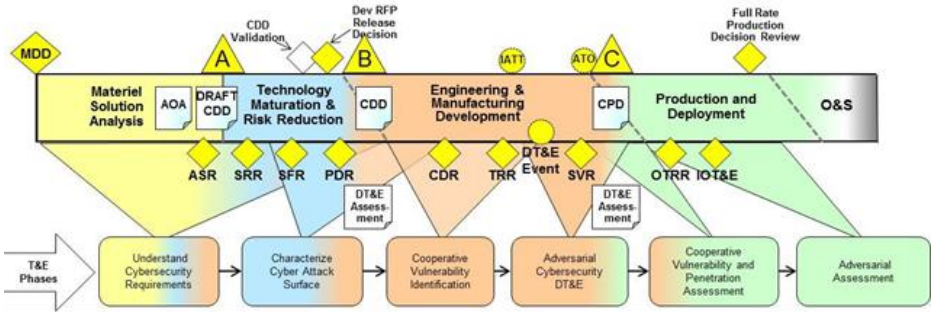

Figure 1. Current 6-step Cyber T&E Process (R*eprinted from Cybersecurity T&E Guidebook, 1 July 2015.)*

Before this guidance, most direction seemed to be biased toward addressing network IT rather than the systems and software characteristic of weapon systems. The term platform

information technology (PIT) was coined to reference this disconnect, but DOD guidance still remained more tailored to network infrastructures rather than aircraft and similar PIT systems. While the *Cybersecurity T&E Guidebook* offered guidance for the conducting vulnerability assessments, it failed to mandate three important characteristics. First, the requirement for execution of an FMA was missing. The second missing piece of guidance was that which mandated vulnerability assessments before each acquisition milestone. The last portion of missing guidance was the mandated inclusion of a uniquely-qualified CVA Engineer at every vulnerability assessment.

In recent years, DOD entities have launched numerous efforts to identify and mitigate cyber vulnerabilities. Air Force Materiel Command has empowered the 46th Test Squadron at Eglin and Edwards AFBs to build the expertise needed to conduct the cyber aspects of developmental testing. Separately, a cyber tabletop exercise developed as a cooperative effort among the National Cyber Range, Joint Mission Environment Test Capability office, and the US Navy Naval Air Systems Command. This effort supported the P-8A, Triton, and TacMobile programs which make up the Navy's Maritime Patrol and Reconnaissance System of Systems, and the results of this evaluation will be published later this year as a NAVAIRSYSCOM "Best Practice."[15] Also, Dr. Kamal Jabbour and Dr. Sarah Muccio outlined a 4-step process to achieve mission assurance, and a team led by Dr. Jabbour conducted a recent assessment of the F-35 at Edwards AFB.[16] Mark Stephenson, as part of an Air Force Research Lab (AFRL) team that has been conducting vulnerability assessments for many years, published the *Avionics Cyber Vulnerability Assessment and Mitigation Manual* in 2014. While each effort has been successful, their triumph has not resulted from following DOD guidance, but rather from their inherent access to experts with the deep technical understanding of cyber threats and avionics

integration. Unfortunately, not all efforts were conducted early enough in the acquisition cycle, thus leaving the most positive program impacts unrealized.

Mandatory Functional Mission Analysis

Functional Mission Analyses are a powerful new concept within the DOD, and luckily a comprehensive knowledge of the subject is not necessary for this essay. The reader must only understand that an FMA is a methodical approach to defining minimum requirements for mission accomplishment, rather than relying on parochial feelings that *everything* is equally important.[17] Simply stated, an FMA is executed to *objectively prioritize what is most important.* To fully understand the power of executing an FMA, the F-16 is offered as an oversimplified case study. The F-16 was designed in the mid-1970s as a daytime air superiority fighter. Since then, the aircraft has undergone hundreds of upgrades to its airframe, weapons, hardware, and software to evolve into an all-weather multi-role fighter. While these upgrades addressed requirements for mean-time between failures, maximum range, target tracking, and so on, they rarely included requirements that addressed cyber vulnerabilities. As the F-16 stands today, there could be numerous vulnerabilities waiting to be exploited by adversaries.

With unlimited time and money, the DOD could pursue a strategy that identifies and mitigates *every* potential vulnerability. Unfortunately, money is scarce, and with an ever-advancing cyber threat and global instability on numerous fronts, time is also not on our side. Only the vulnerabilities (when combined with a threat and impact) that exceed the risk threshold deemed acceptable by the mission owner should be addressed. For example, if a vulnerability exists but no negative mission impact occurs, the vulnerability should be left unaddressed. Executing an FMA in each mission area is necessary to allow focused effort on only those vulnerabilities deemed critical for mission accomplishment. To illustrate, the F-16's close air

support mission depends heavily upon the usage of a targeting pod, but rarely uses the aircraft's radar. Conversely, for a mission where air-to-air engagements are likely, the radar is likely *required*, but the targeting pod may be considered *desired*. For a multirole aircraft like the F-16, it's tempting to argue that all systems are "equally" required since F-16 units are usually tasked to support a wide array of missions. While this is true, we must always consider the limitations on time and money. The owning major command (or sister-service equivalent) must prioritize the core capabilities they want assured during wartime.

Continuing with the F-16 example, let us assume the mission owner, Air Combat Command, determined striking moving targets with 500-pound weapons to be the most important task for which they require mission assurance. In this case, the heads-up display (HUD) in the F-16 may not be critical for mission accomplishment. The display is nice to have, but additional pilot training and rules of engagement changes could mitigate and allow for operations without a HUD. Does this mean if an FMA determined the HUD was not required that pilots are no longer able to use it? No. While the probability of HUD failure may be higher in a cyber-contested environment, the consequence of failure was determined negligible, thus the USAF and DOD should not spend crucial time or money "hardening" the F-16 HUD. Continuing with this premise, the radar, radar warning receiver, air-to-air missiles, Joint Helmet Mounted Cuing System, Identification Friend or Foe system, and some other systems may not be deemed *critical* for mission accomplishment. At the most extreme, the primary flight control system may not even be deemed critical for mission accomplishment if the back-up system can operate adequately. While this would be a shock to any F-16 pilot, an objective assessment must be accomplished to determine the minimum set of subsystems required for mission accomplishment.

The counter argument to conducting FMAs lies in the high levels of integration seen on many of today's weapon systems. The F-16 was used as an oversimplified example, but in reality, the system components are so highly integrated that without major system redesign, nearly every subsystem can affect all other systems. With the current avionics implementation of an F-16, a vulnerability to one mission is likely a vulnerability to *all* missions. In spite of this, FMAs should still be conducted as doing so may force developers to provide inherently more secure solutions to warfighting problems. As another simplified example, an FMA may result in the recommendation to implement a federated system where target coordinates bypass all aircraft busses and information is sent directly from a targeting pod to a weapon. Bypassing the avionics bus could negate many concerns associated with the high levels of integration seen on the F-16 and other legacy aircraft. This hypothetical example demonstrates that conducting an FMA could drive discussions which may result in unique solutions to problems facing current and future weapon systems. For decades the DOD has demanded more integration (fusion) of sensors, but the cyber threat to mission assurance now demands we reassess this desire. The FMA is where key experts will debate the advantages and disadvantages of integrated versus federated systems. Ultimately, early conduct of FMAs enables the long sought after "baking in" of mission assurance.

Conducting an FMA is not a trivial task, nor is it exclusively a cyber-related function, but it could greatly affect the success of subsequent CH events. While today's fully integrated systems pose a thorny conundrum, each system dropped from the "critical for mission accomplishment" list during an FMA may greatly reduce the workload of the CH team's assessment. Most importantly, by using FMAs, the CH team could say with greater certainty that the system is assured against cyber threats when accomplishing specific tasks or missions

which were prioritized by the mission owner. Granted, a pilot might have to turn their HUD off or switch to a back-up flight control mode, but they'll have much higher confidence in their ability to accurately employ weapons when needed. Furthermore, implementing FMAs will provide combatant commanders with a higher fidelity assessment of what core missions and tasks would be available in a cyber-contested environment.

Mandatory Cyber Hardening Events

The earlier exploration of cybersecurity guidance revealed a six-step, linear, yet iterative T&E approach (Figure 1). While this guidance clearly stated each phase "may be repeated several times due to changes in the system architecture, new or emerging threats, and changes to the system environment," the overall approach will still prove ineffective as assessments are not accomplished until too late in the acquisition process. Furthermore, changes to system design necessitate recurrent FMAs and vulnerability assessments throughout the acquisition lifecycle. Current guidance should be changed to incorporate CH events prior to each milestone (Figure 2).[18]

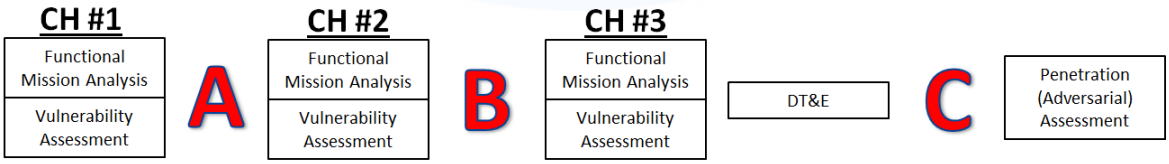

Figure 2. Proposed Cyber T&E Process

Each CH event should include an FMA and a vulnerability assessment. After the FMA identifies the subsystems required for critical mission execution, the vulnerability assessments should include an information flow analysis along with an impact assessment for compromise of the confidentiality, integrity, or availability of information.[19] That is, the team should strive to understand how information is processed, moved, and utilized by the system, and then determine what effects stem from deleting, adding, or changing information. When the effects of "bad"

information are characterized, system modifications or changes to tactics, techniques, and procedures should be used to mitigate the risk to a level deemed acceptable by the mission owner. The following paragraphs describe unique considerations for FMAs and CH events at each milestone.

The first CH event should be conducted prior to Milestone A and should review the overall design philosophy and assess if major, obvious design flaws (vulnerabilities) exist. Since the program is very early in the acquisition timeline, a materiel solution has probably not yet been chosen, and fully understanding system design is highly unlikely. That being said, it is critically important to charter a CH team *early* in the acquisition process even though a developing contractor, government entity, or off-the-shelf solution has not been selected. During this early stage, the CH team should interact with each potential developer to determine if simple, cost-effective, security-enhancing measures could be implemented into proposed designs. For example, the CH team could identify potential areas for tasking AFRL or other technology development entities if engaged prior to Milestone A. Also, the CH team may help inform vendor selection if involved early in the acquisition process.

An FMA conducted early in the process will allow for identification of poor design philosophies and drive discussions which explore the advantages and disadvantages of varying levels of integration. Moving past Milestone A, the second FMA should be repeated only if changes to system design or mission requirements occurred. While changes are often the norm, subsequent FMAs will build on previous ones, so the cost and time for execution should be limited. Prior to Milestone B, the system should be mature enough to enable a much more accurate and detailed review. Early feedback is critical to cost-effectively recommended

changes to current design proposals; waiting too long runs the risk of discovering vulnerabilities that are too costly to fix or too unsecure to field.

Prior to Milestone C, the last CH should be conducted as well as DT&E. The FMA should be a simple task as the system design and mission requirements have likely not experienced major changes. The system design should be nearly complete so the vulnerability assessment will be the highest fidelity yet. Results from this last vulnerability assessment should be presented to the DT&E team and serve as a guide to methodical, rigorous developmental testing. Penetration assessments should not be the focus of DT&E. Testing at this phase should focus on verification of the vulnerability mitigations implemented throughout system development. As an example, if a vulnerability mitigation was implemented to only allow one-way data flow between the radar and a data bus during air-to-air engagements, DT&E should design a test to validate the single-direction flow of information. Time should not be spent trying to identify and exploit attack vectors during DT&E for two main reasons. First and foremost, the inability of the DT&E team to infiltrate the system is not indicative of an adversary's ability to infiltrate the system. Simply stated, we must assume that the adversary hackers are better than ours. Therefore, if DT&E conducted an evaluation, and testers were unable to access the system, a "passing grade" should not necessarily be awarded to the system. Secondly, DT&E should focus on validation and verification of vulnerability mitigations as that line of testing will not otherwise be conducted prior to fielding. If penetration testing is the focus of DT&E, we may never learn that the (hypothetical) "one-way data flow" mitigation *did not work* as designed.

Operational Test and Evaluation (OT&E) should focus on penetration testing. Most of this testing will happen after Milestone C, but some initial tests should be conducted prior to the

last milestone. As is always the case with OT&E, early assessments are encouraged, but any testing conducted prior to the system design being finalized will likely require repeat testing.[20] Similarly, if DT&E occurs prior to the last CH, any subsequent system modifications may require a repeat of test points.

Prior to each milestone, the CH team will provide a risk assessment and recommendations to the Milestone Decision Authority who decides to either advance the program or introduce a delay to further maturity and reduce overall risk. The latter option could add cost to the program or reduce available funds for other enhancements, but may prove to reduce overall cost, as without the recommended changes mission assurance cannot be guaranteed.

Mandatory CVA Engineers

No single factor will prove more important to achieving mission assurance than having the appropriate experts at CH events. Specifically, individuals with deep understandings of operations, system design, avionics integration, information flow analysis, and Byzantine failure analysis must be included. By and large, the success of CH events will hinge upon the inclusion of an expert that the author will term a CVA Engineer.[21] To fully appreciate the uniqueness of this engineer, one must first examine the qualifications of the other team members.

As a baseline for vulnerability assessment team composition, the author relied heavily on the aforementioned Cyber Tabletop vulnerability assessment recently accomplished by the US Navy on the Maritime Patrol and Surveillance System of Systems.[22] The P-8 assessment was completed before Milestone B in April 2015 and successfully identified numerous vulnerabilities before initiation of OT&E. The cornerstone of their success was ensuring the proper people took part in the assessment.[23] The following paragraphs list the CH team members and provide a

brief description of their purpose and duties. The last and most important person listed is the CVA Engineer and will be discussed in greater detail.

Operator – As the end-user of the system, this person brings a deep understanding of tactics, techniques, and procedures to the team. This expert also understands the intent of operations, thus can envision future employment methods.

Operational Tester – This team member will ensure assessments consider operationally relevant situations. This person will best understand how the overall system will be employed in combat. This person may also fill the previous role of "operator."

Developmental Tester – A representative from the DT community shall be present for all CH events. This person will best understand requirements for formulation and adherence to a rigorous process leading up to, and during, DT&E events.

Program Manager – The PM should have the broadest understanding of the entire program, to include how the system works with, and is dependent upon, other systems.

System Engineer – This person best understands how the major pieces of the system are configured and interact with one another.

Software Engineer / Computer Programmer – An expert in specific types of programming language must be present. If more than one language is used, which is often the case, multiple experts may be required unless a single person possesses sufficient expertise in all necessary languages.

Subsystem Engineer / SMEs - An expert in each subsystem (i.e. radar, flight controls, etc.) will be present. There will be more than one of these SMEs on any given program. These experts will have the deepest technical understanding of each subsystem.

CVA Engineer– This is the most critical person at the CH event and should play a leadership role in vulnerability assessments. This person will have a deeply developed skillset that allows them to understand how to not only characterize, but also exploit a cyber-attack surface. They must be proficient at conducting information flow analysis and Byzantine failure analysis on advanced, integrated avionics systems. Without a CVA Engineer, the remaining team members could characterize the overall system of systems, but would be unlikely to see many of the weaknesses in the system design. The adversarial mindset of the CVA Engineer will help the team identify the weaknesses, seams, and limitations of a design.

Unfortunately, the DOD does not have many personnel with the skill sets required of a CVA Engineer. This simple fact will drive the duration that the DOD operates without mission assurance. Only small pockets of DOD expertise exist, in part, because of the military's extreme focus on *network* security rather than *system* security and mission assurance. The focus on network security is also reflected in the mission and great Americans who make up the 24th and 25th Air Forces. These organizations have thousands of experts focused on network operations but do not have personnel with the skills required for vulnerability assessments of major weapon systems. Even the nation's premier cybersecurity experts at the NSA recognized that integrated aircraft systems are far different than traditional IT systems .

This problem has vexed the 46th Test Squadron at Eglin AFB (and their detachment at Edwards AFB) that is responsible for growing a cyber-test capability for weapon systems. DOD leadership should take immediate steps to bolster the numbers of CVA Engineers within the military. In the short term, some service members should cross-train away from their primary career field and into one where duties as a CVA Engineer can be performed and cultivated. Emphasis should be placed on a strong engineering background rather than cyber or

communications career field experience. On-the-job-training with the pockets of experts that already exist could serve as a stop-gap measure. For part of the long-term solution, the DOD should support university programs such as the one led by Dr. Seker at Embry-Riddle Aeronautical University, which aims to fuse the dual knowledge cores of avionics design and cybersecurity.[24] If DOD leadership does not immediately act to secure the high ground of the crossroads between cybersecurity and aviation, someone else will.

Recommendations

The author provides three major recommendations to enable and foster mission assurance across legacy and future weapon systems. These recommendations should be implemented in the next release of DODI 5000.02, *Operation of the Defense Acquisition System*, DODI 8500.01, *Cybersecurity*, and the *Cybersecurity Test and Evaluation Guidebook*.

1. Mandate execution of FMAs on each system before vulnerability assessments.
2. Execute CH events (which include an FMA and vulnerability assessment) before each milestone.
3. Mandate the inclusion of CVA Engineers during all vulnerability assessments.

Conclusion

The DOD should revise guidance to better identify and mitigate cyber vulnerabilities in major weapon systems. First, FMAs will enable more focused, efficient hardening events and will eventually drive mission assurance to be "baked in" to system design. Secondly, conducting discrete CH events before each milestone is fundamental to achieving mission assurance and provides risk assessments the Milestone Decision Authority, who retains the ability to move a program through the acquisition process. Ultimately, the success of these events will hinge on the inclusion of properly qualified CVA Engineers.

Despite implementing these changes, a hurdle still facing the DOD will be the reluctance to spend money on mitigating vulnerabilities that exist in legacy weapon systems. When the warfighter is begging for new capabilities, it is extremely difficult to spend money on an enhancement that is transparent to the end user. For the near future, the acquisition, operational, and requirements communities are well advised to transition from a mindset of, "I want this new widget for my platform," to simply, "I want my platform to work in combat, which will be a cyber-contested environment." Guaranteeing a system is impervious to cyber attack is not feasible in modern warfare, but instituting the author's recommendations will provide warfighters and COCOMs a better chance of success and a clear understanding of at-risk mission areas.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

[1] Kelion, "Fatal A400M Crash."

[2] Gallagher, "Airbus Confirms Software Configuration."

[3] de Briganti, "Airbus Aims at Huge Export Market."

[4] For a further review of the threat and impact to the civilian aviation industry, see AIAA's decision paper "A Framework for Aviation Cybersecurity."

[5] Dr. Kamal Jabbour, Air Force Senior Scientist for Information Assurance, was instrumental in forming the author's understanding of the dual nature of the cyber problem facing weapon systems.

[6] For further discussion on the "how" versus "what" discussion, see Young and Levinson's "Inside Risks: An Integrated Approach to Safety and Security Based on Systems Theory."

[7] Orth, "For Whom Ma Bell Tolls Not," 28.

[8] Freedburg, "Top Official Admits."

[9] Lyngaas, "Exclusive: The OPM Breach."

[10] This description of risk originates with the National Institute of Standards and Technology in Stoneburner, Goguen, and Feringa's *Risk Management Guide for Information Technology Systems* and was further described by Jabbour and Muccio in "On Mission Assurance."

[11] Description of cyber subject matter expert provided by Dr. Kamal Jabbour.

[12] Cyber hardening is not a term widely in use by the DOD. The author presents this term to describe a formal event that includes a functional mission analysis *and* vulnerability assessment.

[13] DODI 5000.02. *Operation of the Defense Acquisition System,* 92, 136.

[14] DODI 8500.01. *Cybersecurity*, 24.

[15] Recognition of report as "Best Practice" provided by Dr. Michael Lilienthal.

[16] Jabbour and Muccio, "The Science of Mission Assurance," 68.

[17] A Functional Mission Analysis is closely related to Systems-Theoretic Process Analysis – Security as presented by Young and Levinson's *Inside Risks: An Integrated Approach to Safety and Security Based on Systems Theory.*

[18] The recommendation to conduct vulnerability assessments earlier in the acquisition process is supported by Hutchinson's 2013 argument to *Shift Left!*

[19] Jabbour and Poisson, *Cyber Vulnerability Assessment: A Primer,* 2016.

[20] Gilmore, *Procedures for Operational Test,* 3.

[21] The term CVA Engineer stems from discussion with 46th Test Squadron personnel that referenced the term Cyber Vulnerability and Penetration Assessment (CVPA) Engineer. The

CVPA moniker acknowledged the close relationship between the skills required to *identify vulnerabilities* and the skills required to *execute penetration assessments*. The author attempts to delineate the skills between the two events by dropping the reference to "penetration assessment" as that should primarily be an OT&E function.

[22] Steinfeld, Pringle, and Lilienthal, "A Mission Based Approach."

[23] Many thanks to Dr. Michael Lilienthal who provided and entertained numerous briefings, phone calls, and e-mails which guided the author towards a better understanding of the social dynamics and team composition of vulnerability assessments.

[23] See Embry-Riddle Aeronautical University's Cybersecurity and Assured Systems Engineering Center website for more information at https://daytonabeach.erau.edu/about/labs/cybase/index.html.

Bibliography

A Framework for Aviation Cybersecurity. AIAA Decision Paper. August 2013.

de Briganti, Giovanni. "Airbus Aims at Huge Export Market for A400M." *Defense-Aerospace.com,* 14 May 2013. http://www.defense-aerospace.com/articles-view/feature/5/144962/airbus-aims-at-huge-a400m-export-market.html (accessed 6 February 2016).

Department of Defense (DOD). *Cybersecurity Test and Evaluation Guidebook,* 1 July 2015.

DOD Instruction 5000.02. *Operation of the Defense Acquisition System,* 7 January 2015.

DOD Instruction 8500.01. *Cybersecurity,* 14 March 2014.

Embry-Riddle Aeronautical University, Daytona Beach Labs and Facilities. "Cybersecurity and Assured Systems Engineering Center." Embry-Riddle Aeronautical University. https://daytonabeach.erau.edu/about/labs/cybase/index.html (accessed 6 February 2016).

Freedburg, Sydney J. Jr. "Top Official Admits F-35 Stealth Fighter Secrets Stolen." *Breakingdefense.com,* 20 June 2013. http://breakingdefense.com/2013/06/top-official-admits-f-35-stealth-fighter-secrets-stolen/ (accessed 6 February 2016).

Gallagher, Sean. "Airbus Confirms Software Configuration Error Caused Plane Crash." *Arstechnica.com,* 1 June 2015. http://arstechnica.com/information-technology/2015/06/airbus-confirms-software-configuration-error-caused-plane-crash/ (accessed 6 February 2016).

Gilmore, J. Michael. *Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs.* Memorandum, 1 August 2014.

Hutchinson, Steven J. "Shift Left!" *International Test and Evaluation Journal* 34, (2013): 133-137.

Jabbour, Kamal T. and Jenny Poisson. "Cyber Vulnerability Assessment: A Primer." White Paper, 28 January 2016.

Jabbour, Kamal T., and Sarah Muccio. "On Mission Assurance." In *Conflict and Cooperation in Cyberspace: The Challenge to National Security,* edited by Yannkogeorgos, Panayotis A., and Adam B. Lowther, 107-126. Boca Raton, FL: Taylor and Francis Group, July 2013.

Jabbour, Kamal T., and Sarah Muccio. "The Science of Mission Assurance." *Journal of Strategic Security* 4, no. 2 (Summer 2011): 61-74.

Kelion, Leo. "Fatal A400M Crash Linked to Data-wipe Mistake." *BBC.com,* 10 June 2015. http://www.bbc.com/news/technology-33078767 (accessed 6 February 2016).

Lyngaas, Sean. "Exclusive: The OPM Breach Details You Haven't Seen." *FCW.com,* 21 August 2015. https://fcw.com/articles/2015/08/21/opm-breach-timeline.aspx (accessed 6 February 2016).

Orth, Maureen. "For Whom Ma Bell Tolls Not." *Los Angeles Times,* 31 October 1971.

Steinfeld, Hank, Paola Pringle, and Michael Lilienthal. "A Mission Based Approach for Analyzing the Risk of Cyber Vulnerabilities." Presentation to 32nd Annual Test and Evaluation Symposium, Arlington, VA: August 2015.

Stoneburner, Gary, Alice Goguen, and Alexis Feringa. *Risk Management Guide for Information Technology,* National Institute of Standards and Technology Special Publication 800-30, July 2002.

Young, William, and Nancy G. Levinson. "Inside Risks: An Integrated Approach to Safety and Security Based on Systems Theory." *Communications of ACM* 57, no. 2 (February 2014): 31-35.